STATE OF SOUTH CAROLINA COUNTY OF CHESTERFIELD JOANN FORD, on behalf of herself and all others similarly situated, Plaintiff, vs. SANDHILLS MEDICAL FOUNDATION, INC., Defendant.	IN THE COURT OF COMMON PLEAS **SUMMONS** **CLASS ACTION COMPLAINT**

TO THE DEFENDANTS ABOVE-NAMED:

YOU ARE HEREBY SUMMONED and required to answer complaint herein, a copy of which herewith served upon you, and to serve a copy of your answer to this complaint upon the subscriber, at the address below, within thirty (30) days after service hereof, exclusive of the day of such service, and if you fail to answer the complaint, judgement by default will be rendered against you for the relief demanded in the complaint.

/s/ Dylan A. Bess
DYLAN A. BESS, ESQ. (SC BAR NO. 101648)
MORGAN & MORGAN, ATLANTA PLLC
P.O. Box 57007
Atlanta, GA 30343-1007
(404) 965-1886
sbrown@forthepeople.com
Attorney for Plaintiff and the Putative Class

June 18, 2021
Chesterfield County, South Carolina

STATE OF SOUTH CAROLINA COUNTY OF CHESTERFIELD JOANN FORD, on behalf of herself and all others similarly situated, Plaintiff, vs. SANDHILLS MEDICAL FOUNDATION, INC., Defendant.	IN THE COURT OF COMMON PLEAS FOURTH JUDICIAL CIRCUIT Civil Action No.: **CLASS ACTION COMPLAINT** DEMAND FOR JURY TRIAL

Plaintiff JoAnn Ford ("Plaintiff"), individually and on behalf of all others similarly situated ("Class Members"), brings this Class Action Complaint against Sandhills Medical Foundation, Inc. ("Defendant" or "Sandhills"), and alleges, upon personal knowledge as to her own actions and her counsels' investigations, and upon information and belief as to all other matters, as follows:

I. INTRODUCTION

1. Plaintiff brings this class action against Defendant for its failure to properly secure and safeguard personally identifiable information that Defendant stored on and/or shared using its vendor's online data storage platform, including, without limitation, names, dates of birth, mailing and email addresses, driver's licenses and state identification cards, and Social Security numbers (collectively, "personally identifiable information" or "PII") as well as claims information that could be used to determine diagnoses/conditions (collectively, "protected health information" or "PHI").[1]

[1] Personally identifiable information generally incorporates information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information. 2 CFR § 200.79. At a minimum, it includes all information that on its face

2. According to Defendant's website, it "provide[s] a wide range of healthcare from treating short term ailments, behavioral health care, to chronic illness such as diabetes and hypertension."[2] Defendant has eight (8) locations, all in South Carolina.[3]

3. Defendant's patients entrust Defendant with an extensive amount of their PII and PHI. Defendant retains this information on computer hardware—even after the relationship ends. Defendant asserts that it understands the importance of protecting such information.

4. On or before January 8, 2021, Defendant learned that an unauthorized actor breached Defendant's vendor's online data storage platform, which Defendant had used to store and/or share the PII and PHI of Plaintiff and Class Members (the "Data Breach").

5. On or before January 8, 2021, Defendant learned that, during the Data Breach, the unauthorized actor exfiltrated the PII and PHI of Plaintiff and Class Members, including, but not limited to, names, dates of birth, mailing and email addresses, driver's licenses and state identification cards, and Social Security numbers as well as claims information that could be used to determine diagnoses/conditions.

6. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' PII and PHI, Defendant assumed legal and equitable duties to those individuals.

7. The exposed PII and PHI of Plaintiff and Class Members can be sold on the dark web. Hackers can access and then offer for sale the unencrypted, unredacted PII and PHI to criminals. Plaintiff and Class Members face a lifetime risk of identity theft, which is heightened

---

expressly identifies an individual. PII also is generally defined to include certain identifiers that do not on their face name an individual, but that are considered to be particularly sensitive and/or valuable if in the wrong hands (for example, Social Security number, passport number, driver's license number, financial account number).

[2] *See* http://sandhillsmedical.org/services/ (last visited May 7, 2021).

[3] *See* http://sandhillsmedical.org/locations/ (last visited May 7, 2021).

here by the loss of Social Security numbers.

8. This PII and PHI was compromised due to Defendant's negligent and/or careless acts and omissions and the failure to protect the PII and PHI of Plaintiff and Class Members.

9. Plaintiff brings this action on behalf of all persons whose PII and PHI was compromised as a result of Defendant's failure to: (i) adequately protect the PII and PHI of Plaintiff and Class Members; (ii) warn Plaintiff and Class Members of its inadequate information security practices; and (iii) avoid sharing the PII and PHI of Plaintiff and Class Members without adequate safeguards. Defendant's conduct amounts to negligence and violates federal and state statutes.

10. Plaintiff and Class Members have suffered injury as a result of Defendant's conduct. These injuries include: (i) lost or diminished value of PII and PHI; (ii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII and PHI; (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time, and significantly (iv) the continued and certainly an increased risk to their PII and PHI, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) may remain backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII and PHI.

11. Defendant disregarded the rights of Plaintiff and Class Members by intentionally, willfully, recklessly, or negligently failing to take and implement adequate and reasonable measures to ensure that Plaintiff's and Class Members' PII and PHI was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required and appropriate protocols, policies and procedures regarding the encryption of data, even for internal use. As the result, the PII and PHI of Plaintiff and Class Members was compromised

through disclosure to an unknown and unauthorized third party. Plaintiff and Class Members have a continuing interest in ensuring that their information is and remains safe, and they should be entitled to injunctive and other equitable relief.

II. PARTIES

12. Plaintiff JoAnn Ford is a citizen of South Carolina residing in Kershaw County, South Carolina.

13. Defendant Sandhills Medical Foundation, Inc. is a South Carolina corporation headquartered at 645 S. 7th Street, McBee, SC 29101, Chesterfield County, South Carolina.

14. Defendant Sandhills Medical Foundation, Inc. is a domestic non-profit with its principal place of business in South Carolina. It can be served with process by serving it's registered agent Christopher W. Dixon at 645 S. 7th Street, McBee, SC 29101, Chesterfield County, South Carolina.

15. The true names and capacities of persons or entities, whether individual, corporate, associate, or otherwise, who may be responsible for some of the claims alleged herein are currently unknown to Plaintiff. Plaintiff will seek leave of court to amend this complaint to reflect the true names and capacities of such other responsible parties when their identities become known.

16. All of Plaintiff's claims stated herein are asserted against Defendant and any of its owners, predecessors, successors, subsidiaries, agents and/or assigns.

III. JURISDICTION AND VENUE

17. This Court has subject-matter jurisdiction over this matter pursuant to Article V, § 11 of the South Carolina Constitution.

18. This Court has personal jurisdiction over Defendant because it is organized under the laws of South Carolina, transacts business in South Carolina, and maintains its principal place of business in South Carolina.

19. Venue is appropriate in this Court under South Carolina Code § 15-7-30 because Chesterfield County (a) was the county in which Defendant had its principal place of business at the time the cause of action arose and (b) is the county where the most substantial part of the acts and omissions giving rise to this cause of action occurred.

IV. FACTUAL ALLEGATIONS

Background

20. Defendant used its vendor's online data storage platform to store some of Plaintiff's and Class Members most sensitive and confidential information, including, but not limited to, names, dates of birth, mailing and email addresses, driver's licenses and state identification cards, and Social Security numbers as well as claims information that could be used to determine diagnoses/conditions, which include information that is static, does not change, and can be used to commit myriad financial crimes.

21. Plaintiff and Class Members relied on this sophisticated Defendant to keep their PII and PHI confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information. Plaintiff and Class Members demand security to safeguard their PII and PHI.

22. Defendant had a duty to adopt reasonable measures to protect Plaintiff's and Class Members' PII and PHI from involuntary disclosure to third parties.

The Data Breach

23. On or about March 5, 2021, Defendant announced that it was subject to the Data

Breach and filed a sample "Notice of Data Breach" with the Attorney General of Maine, which stated as follows:

> **What Happened**
>
> Sandhills Medical Foundation, Inc., contracts with a vendor for online data storage. On January 8, 2021, the vendor notified Sandhills that hackers accessed their system and took Sandhill's' data on or before December 3, 2020. According to the vendor's investigation, the hackers connected to their system on September 23, 2020 and could have accessed Sandhills' data as early as November 15, 2020. The vendor paid a ransom and the hackers returned the data. The hackers told the vendor they deleted the data and did not keep any copies. The vendor's cybersecurity experts monitored the internet and did not find any evidence that the hackers attempted to sell the data.
>
> **What Information Was Involved**
>
> Sandhills determined that patient medical records, lab results, medications, credit card numbers, and bank account numbers were NOT affected. The affected data included demographic information, such as names, dates of birth, mailing and email addresses, driver's licenses and state identification cards, and Social Security numbers. It also included claims information which could be used to determine diagnoses/conditions.
>
> **What We Are Doing**
>
> The vendor reported this incident to law enforcement and worked with cybersecurity experts to address, contain and recover from this incident. The vendor reported that it strengthened its security measures. As described below, Sandhills is also offering you free identity theft protection services.[4]

24. Defendant admitted in the sample notice that an unauthorized party exfiltrated and held for ransom sensitive information about Plaintiff and Class Members, including names, dates of birth, mailing and email addresses, driver's licenses and state identification cards, and Social Security numbers as well as claims information that could be used to determine

[4] Ex. 1 (Sample *Notice of Data Breach*) filed with Maine Attorney's General) at 1.

diagnoses/conditions.

25. In response to the Data Breach, Defendant claims that "the vendor reported that it strengthened its security measures."[5] However, the details of the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure a breach does not occur again have not been shared with regulators or Plaintiff and Class Members, who retain a vested interest in ensuring that their information remains protected.

26. Plaintiff's and Class Members' unencrypted information may end up for sale on the dark web, or simply fall into the hands of companies that will use the detailed PII and PHI for targeted marketing without the approval of Plaintiff and Class Members. Unauthorized individuals can easily access the PII and PHI of Plaintiff and Class Members.

27. Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive, unencrypted information it was maintaining for Plaintiff and Class Members, causing their PII and PHI to be exposed.

Defendant Acquires, Collects and Stores Plaintiff's and Class Members' PII and PHI.

28. Defendant acquired, collected, and stored Plaintiff's and Class Members' PII and PHI.

29. As a condition of its relationships with Plaintiff and Class Members, Defendant required that Plaintiff and Class Members entrust Defendant with highly confidential PII and PHI.

30. By obtaining, collecting, and storing the PII and PHI of Plaintiff and Class Members, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting the PII and PHI from disclosure.

31. Plaintiff and Class Members have taken reasonable steps to maintain the

[5] *Id.*

confidentiality of their PII and PHI and relied on Defendant to keep their PII and PHI confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

Securing PII and PHI and Preventing Breaches

32. Defendant could have prevented this Data Breach by properly securing and encrypting the PII and PHI of Plaintiff and Class Members. Alternatively, Defendant could have destroyed the data, especially decade-old data from former patients.

33. Defendant's negligence in safeguarding the PII and PHI of Plaintiff and Class Members is exacerbated by the repeated warnings and alerts directed to protecting and securing sensitive data.

34. Despite the prevalence of public announcements of data breach and data security compromises, Defendant failed to take appropriate steps to protect the PII and PHI of Plaintiff and Class Members from being compromised.

35. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[6] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[7]

36. The ramifications of Defendant's failure to keep secure the PII and PHI of Plaintiff

[6] 17 C.F.R. § 248.201 (2013).

[7] *Id.*

and Class Members are long lasting and severe. Once PII and PHI is stolen, particularly Social Security numbers, fraudulent use of that information and damage to victims may continue for years.

Value of Personal Identifiable Information

37. The PII of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[8] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web.[9] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[10]

38. Social Security numbers, for example, are among the worst kind of personal information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get

---

[8] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last accessed Apr. 5, 2021).

[9] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, *available at*: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last accessed Apr. 5, 2021).

[10] *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last accessed Apr. 5, 2021).

> calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[11]

39. What is more, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

40. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "The credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[12]

41. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change—name, Social Security number, and date of birth.

42. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the

---

[11] Social Security Administration, *Identity Theft and Your Social Security Number*, *available at*: https://www.ssa.gov/pubs/EN-05-10064.pdf (last accessed Apr. 5, 2021).

[12] Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), *available at*: http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft (last accessed Apr. 5, 2021).

black market."[13]

43. Among other forms of fraud, identity thieves may obtain driver's licenses, government benefits, medical services, and housing or even give false information to police.

44. The PII and PHI of Plaintiff and Class Members was taken by hackers to engage in identity theft or and or to sell it to other criminals who will purchase the PII and PHI for that purpose. The fraudulent activity resulting from the Data Breach may not come to light for years.

45. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII and PHI is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[14]

46. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the PII and PHI of Plaintiff and Class Members, including Social Security numbers and/or dates of birth, and of the foreseeable consequences that would occur if the PII and PHI was compromised, including, specifically, the significant costs that would be imposed on Plaintiff and Class Members a result.

47. Plaintiff and Class Members now face years of constant surveillance of their

---

[13] Time Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), *available at*: https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last accessed Apr. 5, 2021).

[14] *Report to Congressional Requesters*, GAO, at 29 (June 2007), *available at:* https://www.gao.gov/products/gao-07-737 (last accessed Apr. 5, 2021).

financial and personal records, monitoring, and loss of rights. Plaintiff and Class Members are incurring and will continue to incur such damages in addition to any fraudulent use of their PII and PHI.

48. Defendant was, or should have been, fully aware of the unique type and the significant volume of data stored on and/or shared using its vendor's "online data storage" platform, amounting to potentially more than thirty-nine thousand individuals' detailed, personal information and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

49. To date, Defendant has offered Plaintiff and Class Members only one year of "single bureau" credit monitoring and identity theft protection. The offered service is inadequate to protect Plaintiff and Class Members from the threats they face for years to come, particularly in light of the PII and PHI at issue here.

50. The injuries to Plaintiff and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the PII and PHI of Plaintiff and Class Members.

Plaintiff JoAnn Ford's Experience

51. From approximately 2018 to 2019, Plaintiff Ford was a patient at Defendant's location in Lugoff, South Carolina.

52. On or around March 5, 2021, Plaintiff Ford received a Notice of Data Breach from Defendant.[15]

53. After the Data Breach, an unknown and unauthorized individual, using Plaintiff Ford's personally identifiable information, applied for a $500 loan with Security Finance

[15] Ex. 2.

Corporation of South Carolina, which mailed a Fair Credit Reporting and Equal Credit Opportunity Acts Notice to Plaintiff Ford on April 2, 2021.[16]

54. As a result of the Data Breach, Plaintiff Ford spent time dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the Data Breach and self-monitoring her accounts. This time has been lost forever and cannot be recaptured.

55. Additionally, Plaintiff Ford is very careful about sharing her sensitive PII and PHI. She has never knowingly transmitted unencrypted sensitive PII or PHI over the internet or any other unsecured source.

56. Plaintiff Ford stores any documents containing her sensitive PII and PHI in a safe and secure location. Moreover, she diligently chooses unique usernames and passwords for her few online accounts.

57. Plaintiff Ford suffered actual injury in the form of damages to and diminution in the value of her PII and PHI—a form of intangible property that Plaintiff Ford entrusted to Defendant for the purpose of her treatment, which was compromised in and as a result of the Data Breach.

58. Plaintiff Ford suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of her privacy.

59. Plaintiff Ford has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her PII and PHI,

[16] According to its website, "Security Finance offers traditional installment loans, which vary in amount, terms and available ancillary products based on the state of operation and the type of license obtained in that given state." *See* https://www.securityfinance.com/frequently-asked-questions/ (last visited May 24, 2021).

especially her Social Security number, in combination with her name, being placed in the hands of unauthorized third-parties and possibly criminals.

60. Plaintiff Ford has a continuing interest in ensuring that her PII and PHI, which, upon information and belief, remain backed up in Defendant's possession, is protected and safeguarded from future breaches.

V. CLASS ALLEGATIONS

61. Plaintiff brings this nationwide class action on behalf of herself and on behalf of all others similarly situated pursuant to Rule 23 of the South Carolina Rules of Civil Procedure and other applicable law.

62. The Nationwide Class that Plaintiff seek to represent is defined as follows:

> All individuals residing in the United States whose PII or PHI was exposed to an unauthorized party as a result of the Data Breach (the "Nationwide Class").

63. Excluded from the Classes are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to their departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

64. Plaintiff reserves the right to modify or amend the definition of the proposed classes before the Court determines whether certification is appropriate.

65. Numerosity, S.C. R. Civ. P. 23(a)(1): The Nationwide Class (the "Class") is so numerous that joinder of all members is impracticable. Defendant reported to the Attorney General

of Maine that more than 1.4 million individuals were affected by the Data Breach.

66. Commonality, S.C. R. Civ. P. 23(a)(2): Questions of law and fact common to the Classes exist. These include:

a. Whether and to what extent Defendant had a duty to protect the PII and PHI of Plaintiff and Class Members;

b. Whether Defendant had a duty not to disclose the PII and PHI of Plaintiff and Class Members to unauthorized third parties;

c. Whether Defendant had a duty not to use the PII and PHI of Plaintiff and Class Members for non-business purposes;

d. Whether Defendant failed to adequately safeguard the PII and PHI of Plaintiff and Class Members;

e. Whether and when Defendant actually learned of the Data Breach;

f. Whether Defendant adequately, promptly, and accurately informed Plaintiff and Class Members that their PII and PHI had been compromised;

g. Whether Defendant violated the law by failing to promptly notify Plaintiff and Class Members that their PII and PHI had been compromised;

h. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

i. Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

j. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII and PHI of Plaintiff and Class Members;

k. Whether Plaintiff and Class Members are entitled to actual, damages, and/or statutory damages as a result of Defendant's wrongful conduct;

l. Whether Plaintiff and Class Members are entitled to restitution as a result of Defendant's wrongful conduct; and

m. Whether Plaintiff and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

67. Typicality, S.C. R. Civ. P. 23(a)(3): Plaintiff's claims are typical of those of other Class Members because all had their PII and PHI compromised as a result of the Data Breach, due to Defendant's misfeasance.

68. Policies Generally Applicable to the Class: This class action is also appropriate for certification because Defendant has acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members, and making final injunctive relief appropriate with respect to the Class as a whole. Defendant's policies challenged herein apply to and affect Class Members uniformly and Plaintiff's challenge of these policies hinges on Defendant's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiff.

69. Adequacy, S.C. R. Civ. P. 23(a)(4): Plaintiff will fairly and adequately represent and protect the interests of the Class Members in that she has no disabling conflicts of interest that would be antagonistic to those of the other Members of the Class. Plaintiff seeks no relief that is antagonistic or adverse to Class Members and the infringement of the rights and the damages she has suffered are typical of other Class Members. Plaintiff has retained counsel experienced in complex class action litigation, and Plaintiff intends to prosecute this action vigorously.

70. The class litigation is an appropriate method for fair and efficient adjudication of

the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against large corporations, like Defendant. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

71. The nature of this action and the nature of laws available to Plaintiff and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiff and Class Members for the wrongs alleged because Defendant would necessarily gain an unconscionable advantage since it would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiff were exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

72. The litigation of the claims brought herein is manageable. Defendant's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

73. Adequate notice can be given to Class Members directly using information maintained in Defendant's records.

74. Unless a Class-wide injunction is issued, Defendant may continue in its failure to properly secure the PII and PHI of Class Members, Defendant may continue to act unlawfully as set forth in this Complaint.

75. Further, Defendant has acted or refused to act on grounds generally applicable to the Classes and, accordingly, final injunctive or corresponding declaratory relief with regard to the Class Members as a whole is appropriate.

76. Likewise, particular issues are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendant owed a legal duty to Plaintiff and Class Members to exercise due care in collecting, storing, using, and safeguarding their PII and PHI;

b. Whether Defendant breached a legal duty to Plaintiff and Class Members to exercise due care in collecting, storing, using, and safeguarding their PII and PHI;

c. Whether Defendant failed to comply with its own policies and applicable laws, regulations, and industry standards relating to data security;

d. Whether an implied contract existed between Defendant on the one hand, and Plaintiff and Class Members on the other, and the terms of that implied contract;

e. Whether Defendant breached the implied contract;

f. Whether Defendant adequately and accurately informed Plaintiff and Class Members that their PII and PHI had been compromised;

g. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

h. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII and PHI of Plaintiff and Class Members; and,

i. Whether Plaintiff and Class Members are entitled to actual damages, statutory damages, and/or injunctive relief as a result of Defendant's wrongful conduct.

COUNT I
Negligence
(On Behalf of Plaintiff and the Nationwide Class)

77. Plaintiff and the Nationwide Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 76.

78. Plaintiff and the Nationwide Class provided and entrusted Defendant with certain PII and PHI, including their names, dates of birth, mailing and email addresses, driver's licenses and state identification cards, and Social Security numbers as well as claims information that could be used to determine diagnoses/conditions.

79. Plaintiff and the Nationwide Class entrusted their PII and PHI to Defendant on the premise and with the understanding that Defendant would safeguard their information, use their PII and PHI for business purposes only, and/or not disclose their PII and PHI to unauthorized third parties.

80. Defendant has full knowledge of the sensitivity of the PII and PHI and the types of harm that Plaintiff and the Nationwide Class could and would suffer if the PII and PHI were wrongfully disclosed.

81. Defendant knew or reasonably should have known that the failure to exercise due

care in the collecting, storing, and using of the PII and PHI of Plaintiff and the Nationwide Class involved an unreasonable risk of harm to Plaintiff and the Nationwide Class, even if the harm occurred through the criminal acts of a third party.

82. Defendant had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty includes, among other things, designing, maintaining, and testing Defendant's security protocols to ensure that the PII and PHI of Plaintiff and the Nationwide Class in Defendant's possession was adequately secured and protected.

83. Defendant also had a duty to exercise appropriate clearinghouse practices to remove PII and PHI it was no longer required to retain pursuant to regulations, including that of former patients.

84. Defendant also had a duty to have procedures in place to detect and prevent the improper access and misuse of the PII and PHI of Plaintiff and the Nationwide Class.

85. Defendant's duty to use reasonable security measures arose as a result of the special relationship that existed between Defendant and Plaintiff and the Nationwide Class. That special relationship arose because Plaintiff and the Nationwide Class entrusted Defendant with their confidential PII and PHI, a necessary part of their relationships with Defendant.

86. Defendant was subject to an "independent duty," untethered to any contract between Defendant and Plaintiff or the Nationwide Class.

87. A breach of security, unauthorized access, and resulting injury to Plaintiff and the Nationwide Class was reasonably foreseeable, particularly in light of Defendant's inadequate security practices, including sharing and/or storing the PII and PHI of Plaintiff and Class Members on its vendor's "online data storage" platform.

88. Plaintiff and the Nationwide Class were the foreseeable and probable victims of any inadequate security practices and procedures. Defendant knew or should have known of the inherent risks in collecting and storing the PII and PHI of Plaintiff and the Nationwide Class, the critical importance of providing adequate security of that PII and PHI, and the necessity for encrypting PII and PHI stored on Defendant's or its vendor's systems.

89. Defendant's own conduct created a foreseeable risk of harm to Plaintiff and the Nationwide Class. Defendant's misconduct included, but was not limited to, its failure to take the steps and opportunities to prevent the Data Breach as set forth herein. Defendant's misconduct also included its decisions not to comply with industry standards for the safekeeping of the PII and PHI of Plaintiff and the Nationwide Class, including basic encryption techniques freely available to Defendant.

90. Plaintiff and the Nationwide Class had no ability to protect their PII and PHI that was in, and possibly remains in, Defendant's possession.

91. Defendant was in a position to protect against the harm suffered by Plaintiff and the Nationwide Class as a result of the Data Breach.

92. Defendant had and continues to have a duty to adequately disclose that the PII and PHI of Plaintiff and the Nationwide Class within Defendant's possession might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiff and the Nationwide Class to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their PII and PHI by third parties.

93. Defendant had a duty to employ proper procedures to prevent the unauthorized dissemination of the PII and PHI of Plaintiff and the Nationwide Class.

94. Defendant has admitted that the PII and PHI of Plaintiff and the Nationwide Class was wrongfully lost and disclosed to unauthorized third persons as a result of the Data Breach.

95. Defendant, through its actions and/or omissions, unlawfully breached its duties to Plaintiff and the Nationwide Class by failing to implement industry protocols and exercise reasonable care in protecting and safeguarding the PII and PHI of Plaintiff and the Nationwide Class during the time the PII and PHI was within Defendant's possession or control.

96. Defendant improperly and inadequately safeguarded the PII and PHI of Plaintiff and the Nationwide Class in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

97. Defendant failed to heed industry warnings and alerts to provide adequate safeguards to protect the PII and PHI of Plaintiff and the Nationwide Class in the face of increased risk of theft.

98. Defendant, through its actions and/or omissions, unlawfully breached its duty to Plaintiff and the Nationwide Class by failing to have appropriate procedures in place to detect and prevent dissemination of their PII and PHI.

99. Defendant breached its duty to exercise appropriate clearinghouse practices by failing to remove PII and PHI it was no longer required to retain pursuant to regulations, including PII and PHI of former patients.

100. Defendant, through its actions and/or omissions, unlawfully breached its duty to adequately and timely disclose to Plaintiff and the Nationwide Class the existence and scope of the Data Breach.

101. But for Defendant's wrongful and negligent breach of duties owed to Plaintiff and the Nationwide Class, the PII and PHI of Plaintiff and the Nationwide Class would not have been

compromised.

102. There is a close causal connection between Defendant's failure to implement security measures to protect the PII and PHI of Plaintiff and the Nationwide Class and the harm, or risk of imminent harm, suffered by Plaintiff and the Nationwide Class. The PII and PHI of Plaintiff and the Nationwide Class was lost and accessed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such PII and PHI by adopting, implementing, and maintaining appropriate security measures.

103. Additionally, Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect PII and PHI. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

104. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and PHI and not complying with applicable industry standards, as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII and PHI it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiff and the Nationwide Class.

105. Defendant's violation of Section 5 of the FTC Act constitutes negligence *per se*.

106. Plaintiff and the Nationwide Class are within the class of persons that the FTC Act was intended to protect.

107. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and

deceptive practices, caused the same harm as that suffered by Plaintiff and the Nationwide Class.

108. As a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiff and the Nationwide Class have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity of how their PII and PHI is used; (iii) the compromise, publication, and/or theft of their PII and PHI; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII and PHI; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII and PHI, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII and PHI of Plaintiff and the Nationwide Class; and (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII and PHI compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and the Nationwide Class.

109. As a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiff and the Nationwide Class have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

110. Additionally, as a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiff and the Nationwide Class have suffered and will suffer the continued risks of exposure of their PII and PHI, which remain in Defendant's possession and is subject to

further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII and PHI in its continued possession.

111. As a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiff and the Nationwide Class seek actual, consequential, and nominal damages.

COUNT II
Breach of Implied Contract
(On Behalf of Plaintiff and the Nationwide Class)

112. Plaintiff and the Nationwide Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 76.

113. Defendant required Plaintiff and the Nationwide Class to provide and entrust their names, dates of birth, mailing and email addresses, driver's licenses and state identification cards, and Social Security numbers as a condition of being patients of Defendant.

114. As a condition of being patients of Defendant, Plaintiff and the Nationwide Class provided and entrusted their personal information. In so doing, Plaintiff and the Nationwide Class entered into implied contracts with Defendant by which Defendant agreed to safeguard and protect such information, to keep such information secure and confidential, and to timely and accurately notify Plaintiff and the Nationwide Class if their data had been breached and compromised or stolen.

115. Plaintiff and the Nationwide Class fully performed their obligations under the implied contracts with Defendant.

116. Defendant breached the implied contracts it made with Plaintiff and the Nationwide Class by failing to safeguard and protect their personal and financial information and by failing to provide timely and accurate notice to them that personal and financial information was compromised as a result of the data breach.

117. As a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiff and the Nationwide Class have suffered (and will continue to suffer) ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; the illegal sale of the compromised data on the dark web; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts, decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

118. As a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiff and the Nationwide Class seek actual, consequential, and nominal damages.

COUNT III
Invasion of Privacy
(On Behalf of Plaintiff and the Nationwide Class)

119. Plaintiff and the Nationwide Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 76.

120. Plaintiff and the Nationwide Class had a legitimate expectation of privacy to their PII and PHI and were entitled to the protection of this information against disclosure to unauthorized third parties.

121. Defendant owed a duty to its current and former patients, including Plaintiff and the Nationwide Class, to keep their PII and PHI contained as a part thereof, confidential.

122. Defendant failed to protect and released to unknown and unauthorized third parties the PII and PHI of Plaintiff and the Nationwide Class.

123. Defendant allowed unauthorized and unknown third parties access to and

examination of the PII and PHI of Plaintiff and the Nationwide Class, by way of Defendant's failure to protect the PII and PHI.

124. The unauthorized release to, custody of, and examination by unauthorized third parties of the PII and PHI of Plaintiff and the Nationwide Class is highly offensive to a reasonable person.

125. The intrusion was into a place or thing, which was private and is entitled to be private. Plaintiff and the Nationwide Class disclosed their PII and PHI to Defendant as part of Plaintiff' and the Nationwide Class's relationships with Defendant, but privately with an intention that the PII and PHI would be kept confidential and would be protected from unauthorized disclosure. Plaintiff and the Nationwide Class were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

126. The Data Breach at the hands of Defendant constitutes an intentional interference with Plaintiff' and the Nationwide Class's interest in solitude or seclusion, either as to their persons or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

127. Defendant acted with a knowing state of mind when it permitted the Data Breach to occur because it was with actual knowledge that its information security practices were inadequate and insufficient.

128. Because Defendant acted with this knowing state of mind, it had notice and knew the inadequate and insufficient information security practices would cause injury and harm to Plaintiff and the Nationwide Class.

129. As a proximate result of the above acts and omissions of Defendant, the PII and PHI of Plaintiff and the Nationwide Class was disclosed to third parties without authorization,

causing Plaintiff and the Nationwide Class to suffer damages.

130. As a direct and proximate result of Defendant's invasion of privacy, Plaintiff and the Nationwide Class seek actual, consequential, and nominal damages.

131. Unless and until enjoined, and restrained by order of this Court, Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiff and the Nationwide Class in that the PII and PHI maintained by Defendant can be viewed, distributed, and used by unauthorized persons for years to come. Plaintiff and the Nationwide Class have no adequate remedy at law for the injuries in that a judgment for monetary damages will not end the invasion of privacy for Plaintiff and the Nationwide Class.

COUNT IV
Breach of Confidence
(On Behalf of Plaintiff and the Nationwide Class)

132. Plaintiff and the Nationwide Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 76.

133. At all times during Plaintiff' and the Nationwide Class's interactions with Defendant, Defendant was fully aware of the confidential and sensitive nature of Plaintiff' and the Nationwide Class's PII and PHI that Plaintiff and the Nationwide Class provided to Defendant.

134. As alleged herein and above, Defendant's relationship with Plaintiff and the Nationwide Class was governed by terms and expectations that Plaintiff' and the Nationwide Class's PII and PHI would be collected, stored, and protected in confidence, and would not be disclosed to unauthorized third parties.

135. Plaintiff and the Nationwide Class provided their PII and PHI to Defendant with the explicit and implicit understandings that Defendant would protect and not permit the PII and PHI to be disseminated to any unauthorized third parties.

136. Plaintiff and the Nationwide Class also provided their PII and PHI to Defendant with the explicit and implicit understandings that Defendant would take precautions to protect that PII and PHI from unauthorized disclosure.

137. Defendant voluntarily received in confidence the PII and PHI of Plaintiff and the Nationwide Class with the understanding that PII and PHI would not be disclosed or disseminated to the public or any unauthorized third parties.

138. Due to Defendant's failure to prevent and avoid the Data Breach from occurring, the PII and PHI of Plaintiff and the Nationwide Class was disclosed and misappropriated to unauthorized third parties beyond Plaintiff' and the Nationwide Class's confidence, and without their express permission.

139. As a direct and proximate cause of Defendant's actions and/or omissions, Plaintiff and the Nationwide Class have suffered damages.

140. But for Defendant's disclosure of Plaintiff' and the Nationwide Class's PII and PHI in violation of the parties' understanding of confidence, their PII and PHI would not have been compromised, stolen, viewed, accessed, and used by unauthorized third parties. The Data Breach was the direct and legal cause of the theft of Plaintiff' and the Nationwide Class's PII and PHI as well as the resulting damages.

141. The injury and harm Plaintiff and the Nationwide Class suffered was the reasonably foreseeable result of Defendant's unauthorized disclosure of Plaintiff' and the Nationwide Class's PII and PHI. Defendant knew or should have known its methods of accepting and securing Plaintiff' and the Nationwide Class's PII and PHI was inadequate as it relates to, at the very least, securing servers and other equipment containing Plaintiff' and the Nationwide Class's PII and PHI.

142. As a direct and proximate result of Defendant's breach of its confidence with Plaintiff and the Nationwide Class, Plaintiff and the Nationwide Class have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their PII and PHI is used; (iii) the compromise, publication, and/or theft of their PII and PHI; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII and PHI; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII and PHI, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII and PHI of Plaintiff and the Nationwide Class; and (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII and PHI compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and the Nationwide Class.

143. As a direct and proximate result of Defendant's breaches of confidence, Plaintiff and the Nationwide Class have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

144. As a direct and proximate result of Defendant's breaches of confidence, Plaintiff and the Nationwide Class seek actual, consequential, and nominal damages.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of themselves and Class Members, request judgment

against Defendant and that the Court grant the following:

A. For an Order certifying the Nationwide Class and appointing Plaintiff and her Counsel to represent such Class;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of the PII and PHI of Plaintiff and Class Members, and from refusing to issue prompt, complete, any accurate disclosures to Plaintiff and Class Members;

C. For injunctive relief requested by Plaintiff, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class Members, including but not limited to an order:

i. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;

ii. requiring Defendant to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

iii. requiring Defendant to delete, destroy, and purge the personal identifying information of Plaintiff and Class Members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;

iv. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the PII and PHI of Plaintiff and Class Members;

v. requiring Defendant to ensure that appropriate safeguards are in place when

sharing PII or PHI with other entities, including vendors or subcontractors;

vi. requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures;

vii. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiff and Class Members;

viii. requiring Defendant to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

ix. requiring Defendant to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees compliance with Defendant's policies, programs, and systems for protecting personal identifying information; and

x. requiring Defendant to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves;

D. For an award of damages, including actual, nominal, and consequential damages,

as allowed by law in an amount to be determined;

E. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

F. For prejudgment interest on all amounts awarded; and

G. Such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff hereby demand that this matter be tried before a jury.

Date: June 8, 2021

Respectfully Submitted,

/s/ Dylan A. Bess
DYLAN A. BESS, ESQ. (SC BAR NO. 101648)
MORGAN & MORGAN, ATLANTA PLLC
P.O. Box 57007
Atlanta, GA 30343-1007
(404) 965-1886
sbrown@forthepeople.com
Attorney for Plaintiff and the Putative Class